Введение в дискретную математику. Лекция 5 (дискретные и булевы функции). План-конспект

Н. Л. Поляков

1 Функции от n переменных и операция суперпозиции

Функцией от n переменных (также n-арной, n-местной) называется любая функция $f : X^n \to Y$. При этом натуральное число n называется *арностью* функции f. Функции $f : X^n \to X$ также называются n-арными функциями *на множестве* X.

Говорят, что функция h получена из функций $f : X^k \to X$, $g_1 : X^{n_1} \to X$, $g_2 : X^{n_2} \to X$, …, $g_k : X^{n_k} \to X$ с помощью *суперпозиции*, если функция h представляется в виде

$$f(g_1(\chi_1^1, \chi_2^1, \ldots, \chi_{n_1}^1), g_2(\chi_1^2, \chi_2^2, \ldots, \chi_{n_2}^2), \ldots, g_k(\chi_1^k, \chi_2^k, \ldots, \chi_{n_k}^k)),$$

где $\chi_1^1, \chi_2^1, \ldots, \chi_{n_1}^1, \chi_1^2, \chi_2^2, \ldots, \chi_{n_2}^2, \ldots, \chi_1^k, \chi_2^k, \ldots, \chi_{n_k}^k$ есть некоторая последовательность переменных (не обязательно различных).

Пример. Функция $f(x, y, z) = xy + yz$ получена из функций сложения и умножения (например на множестве действительных чисел) с помощью суперпозиции.

Класс функций $\mathcal{F}$ на множестве X (произвольных арностей) называется *функционально замкнутым*, если каждая функция, которая может быть получена с помощью суперозиции из функций, принадлежащих данному классу, вновь принадлежит данному классу.

Пример. Класс всех многочленов от произвольного числа переменных (как функций на множестве $\mathbb{R}$) есть функционально замкнутый класс.

Функция f на множестве X *выражается* через множество $\mathcal{F}$ функций на множестве X (или, как еще говорят, через функции из множества $\mathcal{F}$), если она принадлежит каждому функционально замкнутому классу функций, содержащему $\mathcal{F}$ в качестве подмножества. Иначе говоря, функция f выражается через функции $g_1, g_2, \ldots, g_n$, если она является одной из этих функций или может быть получена из них с помощью суперпозиции (быть может, примененной многократно).

Пример. Функция $u(x, y) = 2xy$ выражается через функции $f(x, y) = x+y$, $g(x, y) = x - y$ и $h(x) = x^2$, поскольку

$$h(x, y) = (x + y)^2 - x^2 - y^2 = g(g(h(f(x, y)), h(x)), h(y)).$$

Для каждого множества X множество всех функционально замкнутых классов функций на множестве X образует решетку по включению. Инфимум двух замкнутых классов это их пересечение, а супремум – наименьший по включению замкнутый класс, который содержит их объединение в качестве подмножества.

2 Дискретные и булевы функции

2.1 Определение и примеры

Классический объект изучения дискретной математики – функции (произвольной арности) на множестве $X = \{0, 1, \ldots, n\}$ или просто на какомлибо конечном множестве. В частном случае, когда $X = \{0, 1\}$ такие функции называются *булевыми*. Любая k-местная булева функция стандартным образом задается таблицей, иногда называемой *таблице истинности*. В первых ее k столбцах перечисляются сверху вниз все последовательности $(x_1, x_2, \ldots, x_k)$ нулей и единиц в лексикографическом порядке, а последний столбец содержит значения $f(x_1, x_2, \ldots, x_k)$. Например, следующая таблица задает булеву функцию трех аргументов:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Подобная стандартизация позволяет избежать лишних записей: k-местную булеву функцию f можно задавать просто последним столбцом ее таблицы истинности (первые k столбцов у всех таких функций совпадают). По соображениям экономии при записи столбец значений транспонируют, т.е. превращают в строку, которая называется вектором значений функции f. В целях еще большей лаконичности вектор значений функции f часто записывают без служебных символов (запятых и скобок). Например, вектор значений функции f из вышеприведенной таблицы есть

$$10011101.$$

Вектор значений трехместной булевой функции есть двоичный вектор длины 8 (по числу возможных наборов значений аргументов). Число всевозможных таких столбцов равно 2^8. Значит, и число различных булевых функций от трех переменных конечно и составляет 2^8. В случае функций от n переменных число строк в таблице равно 2^n , такова же и длина вектора значений, определяющего функцию. Следовательно, число булевых функций от n переменных равно 2^{2^n}. С увеличением числа переменных количество булевых функций быстро нарастает. Так, число булевых функций от одной переменной равно 4, от двух переменных – 16, от трех – 256, от четырех – 65536 и т. д.

Двухместные функции также бывает удобно задавать таблицами, подобными таблицам умножения, например

$\oplus$	0	1
0	0	1
1	1	0

Существует всего четыре булевых функции от одной переменной. все они приведены в следующей таблице.

x	$\mathbf{0}(x)$	$e(x)$	$\overline{x}$	$\mathbf{1}(x)$
0	0	0	1	1
1	0	1	0	1

- $\mathbf{0}(x) = 0$ – функция, тождественно равная 0 (тождественный ноль);
- $e(x) = x$ – тождественная функция;
- $\overline{x} = 1 - x$ – инверсия (или отрицание);
- $\mathbf{1}(x) = 1$ – функция, тождественно равная 1 (тождественная единица).

Все 16 булевых функций от двух переменных вместе с их стандартными обозначениями и названиями приведены в следующей таблице.

x_1	0	0	1	1	
x_2	0	1	0	1	
f_0	0	0	0	0	$\mathbf{0}$ – тождественный ноль
f_1	0	0	0	1	$\cdot$, $\wedge$, пустой символ – умножение, конъюнкция
f_2	0	0	1	0	
f_3	0	0	1	1	x_1 (первая проекция)
f_4	0	1	0	0	
f_5	0	1	0	1	x_2 (вторая проекция)
f_6	0	1	1	0	$\oplus$ – сложение по модулю 2, исключающая дизъюнкция
f_7	0	1	1	1	$\vee$ – дизъюнкция
f_8	1	0	0	0	$\downarrow$ – стрелка Пирса
f_9	1	0	0	1	$\leftrightarrow$ – эквивалентность
f_{10}	1	0	1	0	
f_{11}	1	0	1	1	$\leftarrow$ – обратная импликация
f_{12}	1	1	0	0	
f_{13}	1	1	0	1	$\rightarrow$ — импликация
f_{14}	1	1	1	0	$\mid$ – штрих Шеффера
f_{15}	1	1	1	1	$\mathbf{1}$ – тождественная единица

2.2 Разложение по переменной, СДНФ, СКНФ

Разложение по переменной. Для любой n-местной булевой функции f имеют место формулы разложения по переменной x_i ($1 \leqslant i \leqslant n$):

$$f(x_1, \ldots, x_n) =$$
$$x_i f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \vee \overline{x}_i f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) =$$
$$(x_i \vee f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n))(\overline{x}_i \vee f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n))$$

Это утверждение легко доказывается (упражнение).

СДНФ и СКНФ. Если мы применим это утверждение многократно (пока можно), то получим некоторое стандартное выражение любой булевой функции (кроме тождественного нуля) через дизъюнкцию, конъюнкцию и инверсию, а именно:

$$f(x_1, x_2, \ldots, x_n) = \bigvee_{\substack{\mathbf{s}\in\{0,1\}^n,\\ f(\mathbf{s})=1}} x_1^{s_1} x_2^{s_2} \ldots x_n^{s_n},$$

где $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ и

$$x^{s_i} = \begin{cases} x, & \text{если } s_i = 1, \\ \overline{x}, & \text{если } s_i = 0. \end{cases}$$

Выражение, стоящее в этой формуле справа от знака равенства, называется **совершенной дизъюнктивной нормальной формой** (СДНФ) для функции f. Вообще, совершенная дизъюнктивная нормальная форма от n переменных x_1, x_2, …, x_n это выражение, являющееся дизъюнкцией выражений (*дизъюнктов*), каждое из которых есть конъюнкция переменных x_1, x_2, …, x_n и их инверсий $\overline{x}_1$, $\overline{x}_2$, …, $\overline{x}_n$, такая что каждая переменная входит в эту конъюнкцию ровно один раз (либо непосредственно, либо под символом инверсии).

Двойственная конструкция приводит к представлению любой булевой функции (кроме тождественной единицы) в виде **совершенной конъюнктивной нормальной формы** (СКНФ):

$$f(x_1, x_2, \ldots, x_n) = \bigwedge_{\substack{\mathbf{s}\in\{0,1\}^n,\\ f(\mathbf{s})=0}} x_1^{\overline{s}_1} \vee x_2^{\overline{s}_2} \vee \ldots \vee x_n^{\overline{s}_n},$$

где $\mathbf{s} = (s_1, s_2, \ldots, s_n)$.

Примеры. Пусть функция от трех переменных задана следующей таблицей:

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Тогда
$$f\,(x, y, z) = \overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{y}\,\overline{z} \vee x\,y\,z.$$

Каждый из трех дизъюнктивных членов (слагаемых) записанной формулы соответствует набору значений аргументов, для которого функция принимает значение 1. Каждый дизъюнктивный член содержит все три аргумента функции; отрицанием снабжены те из них, которые имеют значение 0 в соответствующей строке. Так, набору $(0, 0, 0)$ соответствует дизъюнктивный член $\overline{x}\ \overline{y}\ \overline{z}$, набору $(1, 0, 0)$ – дизъюнктивный член $x\overline{y}\ \overline{z}$, набору $(1, 1, 1)$ – дизъюнктивный член xyz.

СКНФ рассмотренной этой функции имеет следующий вид:

$$f(x, y, z) = (x \vee y \vee \overline{z})(x \vee y \vee \overline{z})(x \vee \overline{y} \vee \overline{z})(\overline{x} \vee y \vee \overline{z})(\overline{x} \vee \overline{y} \vee z).$$

Каждый из пяти конъюнктивных членов (множителей) соответствует набору значений аргументов, для которого функция принимает значение 0. Каждый множитель содержит все три аргумента функции; отрицанием снабжены те из них, которые имеют значение 1 в соответствующей строке. Так, набору $(0, 0, 1)$ соответствует множитель $x \vee y \vee \overline{z}$, набору $(0, 1, 0)$ — множитель $x \vee y \vee \overline{z}$, и т. д.

Замечание. Для любой функции f СДНФ (если только f не есть тождественный ноль) и СНКФ (если только f не есть тождественная единица) определяются однозначно с точностью до перестановки дизъюнктов и переменных в каждом дизъюнкте.

Сокращение дизъюнктивных нормальных форм. В общем случае СДНФ и СКНФ булевой функции f это не самое короткое представление функции f с помощью конъюнкции, дизъюнкции и инверсии.

Пример. *Функция большинства* $\mathrm{maj}\,(x, y, z)$ определяется следующей таблицей:

x	y	z	$\mathrm{maj}\,(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Ее СДНФ есть:
$$x\,y\,\overline{z} \vee x\,\overline{y}\,z \vee \overline{x}\,y\,z \vee xyz.$$

Однако, ее можно представить проще:

$$\mathrm{maj}\,(x, y, z) = xy \vee yz \vee xz.$$

Выражения такого типа называются **дизъюнктивными нормальными формами** (ДНФ). Формально, дизъюнктивная нормальная форма от n переменных x_1, x_2, ..., x_n это выражение, являющееся дизъюнкцией выражений (*дизъюнктов*), каждое из которых есть конъюнкция переменных x_1, x_2, ..., x_n и их инверсий $\overline{x}_1$, $\overline{x}_2$, ..., $\overline{x}_n$, такая что каждая переменная входит в эту конъюнкцию **не более одного раза** (либо непосредственно, либо под символом инверсии).[1]

Для преобразования СДНФ булевой функции f (или какой-то другой ДНФ, представляющей функцию f) можно использовать *элементарные преобразования Куайна*

- $Ax \vee A\overline{x} \mapsto Ax \vee A\overline{x} \vee A$, где x – переменная, а A – конъюнкция переменных (неполное склеивание), и

- $Ay \vee A \mapsto A$, где y – переменная, отрицание переменной или пустой символ, а A – конъюнкция переменных (поглощение).

(не забывая про коммутативность и ассоциативность конъюнкции и дизъюнкции).

С помощью многократного применения этих преобразований можно привести ДНФ к такой форме, что дальнейшие преобразования будут уже невозможны. Такая форма называется *сокращенной*. При этом она не обязательно будет кратчайшей. Алгоритмы дальнейшего сокращения дизъюнктивных форм выходят за рамки данного курса.

Для преобразования дизъюнктивных форм вручную можно просто использовать в обе стороны равенства

- $Ax \vee A\overline{x} = A$ и

- $AB \vee A = A$, где B – произвольная (быть может, пустая) конъюнкция.

Но этот метод далек от явного алгоритма и требует догадок.

Пример.

$$\begin{aligned} xy\overline{z} \vee x\overline{y}z \vee \boxed{\overline{x}yz \vee xyz} &= xy\overline{z} \vee x\overline{y}z \vee \boxed{yz} \\ &= xy\overline{z} \vee \boxed{x\overline{y}z \vee xyz} \vee yz \\ &= xy\overline{z} \vee \boxed{xz} \vee yz \\ &= \boxed{xy\overline{z} \vee xyz} \vee xz \vee yz \\ &= xy \vee xz \vee yz. \end{aligned}$$

[1] Симметричным образом определяется понятие **конъюнктивной нормальной формы** (ДНФ).

3 Полные системы функций и критерий Поста.

Полной системой булевых функций называется любое множество булевых функций, через которое могут быть выражены *все* булевы функции с помощью суперпозиции. Из результатов предыдущего раздела следует, что система $\{\wedge, \vee, {}^{-}\}$ есть полная система. Кроме того, если вспомнить, что дизъюнкция выражается через конъюнкцию и инверсию, а конъюнкция выражается через дизъюнкцию и инверсию, можно мгновенно установить, что системы $\{\wedge, {}^{-}\}$ и $\{\vee, {}^{-}\}$ тоже полные.

Как установить, что система функций полная? На этот вопрос отвечает **критерий Поста.**

Специальные классы булевых функций. Определим следующие специальные классы булевых функций.

1. T_0 – класс всех булевых функций, *сохраняющих ноль*, т.е. всех функций $f : \{0,1\}^n \to \{0,1\}$, удовлетворяющих условию:

   $$f(0, 0, \ldots, 0) = 0.$$

   Примеры: 0, $\vee$, $\wedge$, maj, $\oplus$.

2. T_1 – класс всех булевых функций, *сохраняющих единицу*, т.е. всех функций $f : \{0,1\}^n \to \{0,1\}$, удовлетворяющих условию:

   $$f(1, 1, \ldots, 1) = 1.$$

   Примеры: 1, $\vee$, $\wedge$, maj, $\to$.

3. M – класс всех *монотонных* булевых функций. Функция $f : \{0,1\}^n \to \{0,1\}$ называется монотонной, если удовлетворяет условию:

   если $x_1 \leqslant y_1$ и $x_2 \leqslant y_2$ и … и $x_n \leqslant y_n$, то $f(x_1, x_2, \ldots, x_n) \leqslant f(y_1, y_2, \ldots, y_n)$.

   Примеры: $\vee$, $\wedge$, maj.

4. S – класс всех *самодвойственных* булевых функций. Функция $f^* : \{0,1\}^n \to \{0,1\}$ называется двойственной для функции $f : \{0,1\}^n \to \{0,1\}$, если

   $$f^*(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)}.$$

   Пример: дизъюнкция двойственна конъюнкции (и наоборот).
   Булева функция называется самодвойственной, если $f^* = f$.
   Примеры: ${}^{-}$, maj, $f(x, y, z) = x \oplus y \oplus z$.

5. L – класс всех *линейных* булевых функций. Функция $f : \{0,1\}^n \to \{0,1\}$ называется линейной, если она представляется в виде:

   $$f(x_1, x_2, \ldots, x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_n x_n,$$

   где $\alpha_0, \alpha_1, \ldots, \alpha_n \in \{0,1\}$.

Теорема (критерий Поста). Каждый функционально замкнутый класс булевых функций, не совпадающий с множеством всех булевых функций, есть подмножество одного (или нескольких) из классов T_0, T_1, M, S, L. Следовательно, класс булевых функций является полным тогда и только тогда, когда не включен (в качестве подмножества) ни в один из классов T_0, T_1, M, S, L.

Примеры. Следующие классы полны:

- $\{^-, \to\}$,
- $\{\oplus, \wedge, 1\}$,
- $\{\downarrow\}$ (напоминание: $\downarrow$ – стрелка Пирса).

4 Для самостоятельного изучения: полиномы Жегалкина.

Полином Жегалкина это «многочлен» (т.е. унифицированная запись терма, построенного с помощью сложения, умножения и констант) от n переменных, в котором роль сложения играет операция $\oplus$ (т.е. сложение по модулю 2), а коэффициенты берутся из множества $\{0, 1\}$. Поскольку $xx = x$, в записи любого многочлена Жегалкина уместно оставлять только произведения вида $x_{i_1} x_{i_2} \ldots x_{i_k}$, где номера $i_1, i_2, \ldots, i_k$ попарно различны. Таким образом, можно считать, что для любого числа n существует только конечное (а именно, 2^{2^n}) число многочленов Жегалкина от n переменных, и степени таких многочленов не превосходят n.

Общий вид полинома Жегалкина $p(x_1, x_2, \ldots, x_n)$ от n переменных есть

$$a_0 \oplus \bigoplus_{1 \leqslant i \leqslant n} a_i x_i \oplus \bigoplus_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n.$$

Например, общий вид полинома Жегалкина от трех переменных есть

$$a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus a_{12} x_1 x_2 \oplus a_{23} x_2 x_3 \oplus a_{13} x_1 x_3 \oplus a_{123} x_1 x_2 x_3.$$

В выражениях такого вида часто вместо $\oplus$ записывают просто $+$, а вместо $\bigoplus$ просто $\sum$ (если нет опасности перепутать эти операции с обычным суммированием чисел).

Каждую булеву функцию f можно представить в виде полинома Жегалкина. Это делается следующим образом. Если дано представление функции f через какие-то простейшие операции (например, дизъюнкцию, конъюнкцию и отрицание), то, надо использовать выражение этих операций через $\oplus$, $\wedge$ и константы $0, 1$, и раскрыть скобки, помня, что $xx = x$ и $x \oplus x = 0$. Особенно часто используются формулы

$$\begin{aligned} \overline{x} &= x \oplus 1, \\ x \vee y &= x \oplus y \oplus xy. \end{aligned}$$

Пример.

$$\begin{aligned} x_1 \to x_2 &= \overline{x}_1 \vee x_2 \\ &= \overline{x}_1 \oplus x_2 \oplus \overline{x}_1 x_2 \\ &= x_1 \oplus 1 \oplus x_2 \oplus (x_1 \oplus 1) x_2 \\ &= x_1 \oplus 1 \oplus x_2 \oplus x_1 x_2 \oplus x_2 \\ &= 1 \oplus x_1 \oplus x_1 x_2. \end{aligned}$$

Если известна таблица значений функции f, то полином Жегалкина можно найти с помощью *метода неопределенных коэффициентов*. Пусть функция f n-местная. Тогда надо записать общий вид полинома Жегалкина от n переменных, а затем подставить в полученный терм каждый набор $(a_1, a_2, \ldots, a_n) \in \{0, 1\}^n$ и приравнять значению $f(a_1, a_2, \ldots, a_n)$. Получится система из 2^n линейных уравнений с 2^n неизвестными (коэффициентами). Можно показать, что эта система всегда имеет решение. Более того, особый (треугольный) вид этой системы позволяет находить коэффициенты последовательно: из первого уравнения можно найти $a_0 = f(0, 0, \ldots, 0)$, затем подставив найденное значение во второе уравнение, можно найти a_2 и т.д.

Пример. Таблица истинности для функции $\to$ есть

x	y	$x \to y$
0	0	1
0	1	1
1	0	0
1	1	1

Общий вид полинома Жегалкина $p(x_1, x_2)$ есть

$$a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_{12} x_1 x_2.$$

Имеем систему

$$\left\{ \begin{array}{ccccccccccccccccc} a_0 & \oplus & a_1 \cdot 0 & \oplus & a_2 \cdot 0 & \oplus & a_{12} \cdot 0 \cdot 0 & = & a_0 & & & & & & & = & 1 \\ a_0 & \oplus & a_1 \cdot 0 & \oplus & a_2 \cdot 1 & \oplus & a_{12} \cdot 0 \cdot 1 & = & a_0 & \oplus & & & a_2 & & & = & 1 \\ a_0 & \oplus & a_1 \cdot 1 & \oplus & a_2 \cdot 0 & \oplus & a_{12} \cdot 1 \cdot 0 & = & a_0 & \oplus & a_1 & & & & & = & 0 \\ a_0 & \oplus & a_1 \cdot 0 & \oplus & a_2 \cdot 0 & \oplus & a_{12} \cdot 0 \cdot 0 & = & a_0 & \oplus & a_1 & \oplus & a_2 & \oplus & a_{12} & = & 1 \end{array} \right.$$

Решая систему, последовательно находим

$$\begin{aligned}
&a_0 = 1,\\
&1 \oplus a_2 = 1 \Rightarrow a_2 = 0,\\
&1 \oplus a_1 = 0 \Rightarrow a_1 = 1,\\
&1 \oplus 1 \oplus 0 \oplus a_{12} = 1 \Rightarrow a_{1,2} = 1.
\end{aligned}$$

Окончательно, $x_1 \to x_2 = 1 \oplus x_1 \oplus x_1 x_2$.

Есть и явные формулы для коэффициентов полинома Жегалкина. Для каждого индекса $\iota = \alpha_1\alpha_2\ldots\alpha_k \neq 0$ коэффициента в записи общего вида полинома Жегалкина от n переменных обозначим символом $v(\iota)$ характеристический вектор подмножества $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ множества $\{1, 2, \ldots, n\}$. Положим $v(0) = (0, 0, \ldots, 0)$. Тогда для каждого коэффициента a_ι полинома Жегалкина n-местной функции f выполнено:

$$a_\iota = \bigoplus_{\mathbf{x}\in(E_2)^n,\, \mathbf{x}\preccurlyeq v(\iota)} f(\mathbf{x}),$$

где

$$(a_1, a_2, \ldots, a_n) \preccurlyeq (b_1, b_2, \ldots, b_n) \Leftrightarrow a_1 \leqslant b_1 \text{ и } a_2 \leqslant b_2 \text{ и } \ldots \text{ и } a_n \leqslant b_n.$$

Пример. Найдем полином Жегалкина для функции $\to$ с помощью непосредственного вычисления коэффициентов.

ι	$v(\iota)$	a_ι
0	$(0,0)$	$a_0 = (0 \to 0) = 1$
1	$(1,0)$	$a_1 = (0 \to 0) \oplus (1 \to 0) = 1 \oplus 0 = 1$
2	$(0,1)$	$a_2 = (0 \to 0) \oplus (0 \to 1) = 1 \oplus 1 = 0$
12	$(1,1)$	$a_{12} = (0 \to 0) \oplus (0 \to 1) \oplus (0 \to 1) \oplus (1 \to 1) = 1 \oplus 1 \oplus 0 \oplus 1 = 1$

Вновь имеем $x_1 \to x_2 = 1 \oplus x_1 \oplus x_1 x_2$.

5 Для самостоятельного изучения: булевы векторы и матрицы.

Характеристические векторы. Конечные множества, соответствия и отношения можно кодировать двоичными векторами и матрицами. При этом операции над множествами преобразуются в естественные операции над их кодами. Пусть дано конечное множество Ω, занумерованное натуральными числами: $\Omega = \{a_1, a_1, \ldots, a_n\}$. Характеристическим вектором подмножества $A \subseteq \Omega$ называется последовательность (вектор) $\mathbf{u}_A = (u_1, u_2, \ldots, u_n) \in \{0,1\}^n$, для которого

$$u_i = \begin{cases} 1, & \text{если } a_i \in A,\\ 0, & \text{иначе} \end{cases}$$

Пример. Вектор $\{1, 0, 1\}$ есть характеристический вектор подмножества $\{1, 3\}$ множества $\{1, 2, 3\}$, занумерованного в естественном порядке.

Для двоичных векторов одной размерности определены операции поэлементной булевой дизъюнкции и конъюнкции. Кроме того, для любого двоичного вектора определена операция булева отрицания (инверсии).

Если даны логические векторы $\mathbf{u} = (u_1, u_1, \ldots, u_n), \mathbf{v} = (v_1, v_1, \ldots, v_n) \in \{0, 1\}^n$, то

$$\begin{aligned}
&\mathbf{u} \vee \mathbf{v} = (u_1 \vee v_1, u_2 \vee v_2, \ldots, u_n \vee v_n)\\
&\mathbf{u} \wedge \mathbf{v} = (u_1 \wedge v_1, u_2 \wedge v_2, \ldots, u_n \wedge v_n)\\
&\overline{\mathbf{u}} = (\overline{u}_1, \overline{u}_2, \ldots, \overline{u}_n).
\end{aligned}$$

Пример.

$$(1, 0, 1) \vee (0, 1, 1) = (1, 1, 1), \quad (1, 0, 1) \wedge (0, 1, 1) = (0, 0, 1), \quad \overline{(1, 0, 1)} = (0, 1, 0).$$

Для всех подмножеств A, B занумерованного конечного множества Ω выполнено:

$$\mathbf{u}_{A \cup B} = \mathbf{u}_A \vee \mathbf{u}_B \quad \mathbf{u}_{A \cap B} = \mathbf{u}_A \wedge \mathbf{u}_B \quad \mathbf{u}_{\overline{A}} = \overline{\mathbf{u}}_A.$$

Пример. Подмножества $A = \{0, 3\}$ и $B = \{0, 2\}$ множества $\Omega = \{0, 1, 2, 3, 4\}$, занумерованного в естественном порядке, имеют характеристические векторы $(1, 0, 0, 1, 0)$ и $(1, 0, 1, 0, 0)$ соответственно. Тогда множество $A \cup B$ имеет характеристический вектор $(1, 0, 0, 1, 0) \vee (1, 0, 1, 0, 0) = (1 \vee 1, 0 \vee 0, 0 \vee 1, 1 \vee 0, 0 \vee 0) = (1, 0, 1, 1, 0)$. Значит, $A \cup B = \{0, 2, 3\}$ (конечно, это можно было установить и непосредственно).

Характеристические матрицы. Пусть даны конечные множества X и Y, занумерованное натуральными числами:

$$X = \{x_1, x_2, \ldots, x_n\}, \quad Y = \{y_1, y_2, \ldots, y_m\}$$

Характеристической матрицей соответствия R из множества X в множество Y называется двоичная матрица $A = A_R$ размера $n \times m$, для которой

$$a_{ij} = \begin{cases} 1, & \text{если } (x_i, y_j) \in R, \\ 0, & \text{иначе} \end{cases}$$

Пример. Пусть $X = \{x_1, x_2, x_3\}, Y = \{y_1, y_2\}, R = \{(x_1, y_1), (x_1, y_2), (x_3, y_1)\}$. Тогда $A_R = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Для двоичных матриц одной и той же размерности тоже определены операции покомпонентной булевой дизъюнкции и конъюнкции, а для любой булевой матрицы определена операция булева отрицания (инверсии). Если даны логические матрицы A и B одной и той же размерности, то матрицы $C = A \vee B$, $D = A \wedge B$, $F = \overline{A}$ это матрицы той же размерности, причем

$$c_{ij} = a_{ij} \vee b_{ij}, \quad d_{ij} = a_{ij} \wedge b_{ij}, \quad f_{ij} = \overline{a}_{ij}$$

Пример.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \vee \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \wedge \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$
$$\overline{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Кроме того, для двоичных векторов и матриц вводятся операции логического умножения. Если дана двоичная матрица A размера $m \times n$ и двоичный вектор $\mathbf{u} = (u_1, u_2, \ldots, u_m)$, то $\mathbf{u} \circ A$ есть двоичный вектор $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, для которого

$$v_i = (u_1 \wedge a_{1i}) \vee (u_2 \wedge a_{2i}) \vee \ldots \vee (u_m \wedge a_{mi}).$$

Пример.

$$(0,1,1) \circ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = (0,1).$$

Если даны двоичные матрицы A размера $m \times k$ и B размера $k \times n$, то матрица $A \circ B$ есть матрица C размера $m \times n$, для которой

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{km}).$$

Пример.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Наконец, для всех двоичных матриц определена операция транспонирования.

Пример.

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Для любых соответствий R, Q из множества X в множество Y, множества $C \subseteq X$ и соответствия P из множества Y в множество Z

$$\begin{array}{lll} A_{R\cup Q} = A_R \vee A_Q, & A_{R\cap Q} = A_R \wedge A_Q, & A_{\overline{R}} = \overline{A_R} \\ \mathbf{u}_{R(C)} = \mathbf{u}_C \circ A_R, & A_{R\circ P} = A_R \circ A_P, & A_{R^{-1}} = (A_R)^{\mathrm{T}} \end{array}$$

Пример. Используя характеристическую матрицу соответствия

$$R = \{(a,b),(a,c),(b,f),(c,c),(c,b)\}$$

из множества $X = \{a,b,c\}$ в множество $Y = \{b,c,d,e,f\}$, найти образ множества $A = \{a,c\}$.

Решение. Если множества X и Y занумерованы в естественном порядке, то характеристическая матрица соответствия R равна $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$, а характеристический вектор множества $\{a, c\}$ есть $(1, 0, 1)$. Вычисляем

$$(1, 0, 1) \circ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} = (1, 1, 0, 0, 0).$$

Значит, $R(\{a, c\}) = \{b, c\}$.

6 Задачи

1. Постройте таблицу истинности булевой функции
   (a) $f(x, y, z) = (x \oplus (y \to z)) \vee ((y \to z) \to x)$,
   (b) $f(x, y, z)$, которая принимает значение 1 тогда и только тогда, когда $3x + 5y + 2z \geqslant 6$,
   (c) $f(x, y, z)$, которая принимает значение 0 тогда и только тогда, когда тройка (x, y, z) содержит четное число нулей,
   (d) $f(x_1, x_2, x_3, x_4)$, которая принимает значение 1 тогда и только тогда, когда $x_1 + x_2 + x_3 = x_4$ или кортеж (x_1, x_2, x_3, x_4) содержит единиц строго больше, чем нулей.
   (e) $f(x_1, x_2, x_3)$, которая задана вектором значений 00111101.
2. Используя истинностные таблицы, докажите тождества:
   (a) $x \to (y \to x) = 1$.
   (b) $x \to (y \to z) = (x \to y) \to (x \to z)$.
   (c) $\overline{x} \downarrow \overline{y} = xy$.
3. Найдите СДНФ и СКНФ функций из задачи 1.
4. Найдите СДНФ и СКНФ функций:
   (a) $x \mid y$.
   (b) $x \leftrightarrow (y \vee z)$.
   (c) $\operatorname{maj}(\overline{x}, y, z)$.
5. Упростите следующие ДНФ:
   (a) $\overline{x}\, y\, z \vee \overline{x}\, \overline{y}\, z \vee x\, y\, z$.
   (b) $\overline{x}_1\, \overline{x}_2\, \overline{x}_3\, \overline{x}_4 \vee \overline{x}_1\, \overline{x}_2\, \overline{x}_3\, x_4 \vee \overline{x}_1\, \overline{x}_2\, x_3\, \overline{x}_4 \vee \overline{x}_1\, x_2\, x_3\, \overline{x}_4 \vee x_1\, x_2\, x_3\, \overline{x}_4 \vee x_1\, x_2\, x_3\, x_4$.
6. Перечислите все монотонные булевы функции от двух переменных.

7. ($*$) Докажите, что булева функция f, отличная от тождественного нуля и тождественной единицы, монотонна тогда и только тогда, когда выражается через дизъюнкцию и конъюнкцию (иначе говоря, представляется дизъюнктивной нормальной формой без инверсий).

8. Постройте таблицу истинности функции f^* двойственной к функции

   (a) $f(x, y, z) = (x \oplus y) \vee (z \to x)$,

   (b) $f(x_1, x_2, x_3)$ с таблицей истинности

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

   (c) $f(x_1, x_2, x_3)$ с вектором значений 11000011.

9. Постройте таблицу истинности булевой функции f, если известно, что

$$\begin{array}{cccc} f(0,0,0) = 1 & f(0,0,1) = 1 & f(0,1,0) = 0 & f(1,0,0) = 0 \\ f^*(0,0,0) = 0 & f^*(0,0,1) = 0 & f^*(0,1,0) = 1 & f^*(1,0,0) = 1 \end{array}$$

10. Приведите пример булевой функции от двух переменных, для которой

$$f = \overline{f^*}.$$

11. Докажите, что функция большинства $\mathrm{maj}\,(x, y, z)$ самодвойственна.

12. Какому условию должна удовлетворять линейная булева функция $f(x_1, x_2, \ldots, x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_n x_n$, чтобы она была самодвойственной?

13. Найдите линейную булеву функцию f от трех переменных, для которой

$$f(0,1,0) = 1,\ f(0,0,1) = 0,\ f(1,1,1) = 1,\ f(1,0,1) = 1.$$

14. Используя критерий Поста, проверьте полноту следующих классов:

   (a) $\{\to, 0\}$,

   (b) $\{\to, 1\}$,

   (c) $\{\to, \oplus\}$,

   (d) $\{^-, \mathrm{maj}\}$,

   (e) $\{\oplus, \mathrm{maj}, 1\}$,